IN THE CLAIMS

Please amend the claims to read as follows:

Listing of Claims

1. (Currently Amended) A system for providing authentication over a network using a pre-established communications pipe, comprising at least one client, at least one PSD, at least one first remote computer system, at least one subsequent remote computer system, and at least one network wherein said network includes means for functionally connecting and communicating with at least one client and one or more remote computer systems,

said at least one client, further comprising:

means for functionally connecting to a PSD Interface and said network, means for functionally communicating over said network with said first remote computer system and means for establishing a communications pipe; said means for establishing a communications pipe comprising:

client communications means for transmitting and receiving message packets over said network using a packet based communications protocol, and for transmitting and receiving APDUs through said PSD Interface,

first client data processing means for receiving

incoming message packets from said first remote computer system using said client communications means, separating encapsulated APDUs from said incoming message packets thus generating ~~desencapsulated~~ decapsulated APDUs and routing said ~~desencapsulated~~ decapsulated APDUs to said PSD through said PSD Interface independently of the origin and integrity of said incoming message packets, and

second client data processing means for receiving incoming APDUs from said PSD interface, encapsulating said incoming APDUs into outgoing message packets and routing said outgoing message packets to said first remote computer system through said client communications means;

means for transferring incoming commands sent from said first remote computer system through said established communications pipe to said PSD; and

means for transferring outgoing responses generated by said PSD to said first remote computer through said established communications pipe;

said at least one PSD further comprising;

at least one embedded PSD authenticating means,

means to respond to at least one incoming command,

means to generate an outgoing authentication response, and

cryptography means for decrypting said incoming commands and encrypting said outgoing responses, wherein said PSD is functionally connected and is functionally communicating with said client and said first remote computer system;

said at least one first remote computer system further comprising;

means for generating outgoing commands in a proper protocol for communicating with said PSD through said established communications pipe,

a first authenticating means for authenticating said PSD responses,

cryptography means for decrypting said incoming responses and encrypting said outgoing commands,

processing and routing means for transferring authentication challenges received over said network from said subsequent remote computer system to said PSD for authentication through said established communications pipe, and

processing and routing means for transferring authentication responses received through said established communications pipe from said PSD to said subsequent remote computer system over said network,

wherein said first remote computer system is functionally connected to said network and is functionally communicating with

said client and said PSD using said established communications pipe; and

said at least one subsequent remote computer system further comprising:

means to generate authentication challenges, and

a second authenticating means for authenticating responses received over said network from said PSD through said first remote computer system, wherein said subsequent remote computer system is functionally connected to said network and is functionally communicating with said first remote computer system.

2. (Currently Amended) A system for providing authentication over a network using a pre-established communications pipe, comprising at least one client, at least one PSD, at least one first remote computer system, at least one subsequent remote computer system, and at least one network wherein said network includes means for functionally connecting and communicating with at least one client and one or more remote computer systems,

said at least one client, further comprising;

means for functionally connecting to a PSD Interface and said network, means for functionally communicating over said

network with said first remote computer system and means for establishing a communications pipe; said means for establishing a communications pipe comprising:

client communications means for transmitting and receiving message packets over said network using a packet based communications protocol, and for transmitting and receiving APDUs through said PSD Interface,

first client data processing means for receiving incoming message packets from said first remote computer system using said client communications means, separating encapsulated APDUs from said incoming message packets thus generating ~~desencapsulated~~ decapsulated APDUs and routing said ~~desencapsulated~~ decapsulated APDUs to said PSD through said PSD Interface independently of the origin and integrity of said incoming message packets, and

second client data processing means for receiving incoming APDUs from said PSD interface, encapsulating said incoming APDUs into outgoing message packets and routing said outgoing message packets to said first remote computer system through said client communications means;

means for transferring incoming commands sent from said first remote computer system through said established communications pipe to said PSD; and

means for transferring outgoing responses generated by said PSD to said first remote computer through said established communications pipe;

said at least one PSD further comprising:

at least one embedded PSD authenticating means,

means to respond to at least one incoming command,

means to generate an outgoing authentication response,

means to transfer said authenticating means through said client to said first remote computer system, and

cryptography means for decrypting said incoming commands and encrypting said outgoing responses, wherein said PSD is functionally connected and is functionally communicating with said client and said first remote computer system;

said at least one first remote computer system further comprising:

means for generating outgoing commands in a proper protocol for communicating with said PSD through said established communications pipe,

a first authenticating means for authenticating said PSD responses,

cryptography means for decrypting said incoming responses and encrypting said outgoing commands,

storage means for storing said authenticating means

transferred from said PSD, and

a second authenticating means using said PSD authenticating means to provide authentication response to said subsequent remote computer system, wherein said first remote computer system is functionally connected to said network and is functionally communicating with said client and said PSD using said established communications pipe; and

said at least one subsequent remote computer system further comprising:

means to generate authentication challenges,

a third authenticating means for authenticating responses received over said network from said first remote computer system, wherein said subsequent remote computer system is functionally connected to said network and is in functional communications with said first remote computer system.

3. (Original) The system according to claim 1 or 2 wherein said communications employs an open protocol.

4. (Original) The system according to claim 1 or 2 wherein said communications employs a secure protocol.

5. (Original) The system according to claim 1 or 2 wherein said cryptography employs asynchronous methods.

6. (Original) The system according to claim 1 or 2 wherein said cryptography employs synchronous methods.

7. (Currently Amended) A method for providing authentication over a network using a pre-established communications pipe comprising;

establishing a communications pipe between a PSD and a first remote computer system over at least one network and using a client as a communications host for said PSD, wherein said client and said first remote computer system are in functional communication using a packet based communications protocol over said network, and wherein transmitting a first message from said first remote computer system to said PSD through said communications pipe

comprises:

generating said first message on said first remote computer system, wherein said first message is in a non-native protocol for communicating with said PSD and said first message is generated by an API Level Program,

converting on said remote computer system said first message

from said non-native protocol into a first APDU format message using a first server data processing means,

encapsulating on said first remote computer system said first APDU format message into said packet based communications protocol producing a first encapsulated message, using a second server data processing means,

transmitting said first encapsulated message over said network using said packet based communications protocol,

receiving by said client said first encapsulated message sent over said network, processing said first encapsulated message using a first data processing means to separate said first APDU format message from said first encapsulated message,

routing on said client said first APDU format message through a hardware device port assigned to a PSD Interface independently of the origin and integrity of said first encapsulated message, wherein said PSD Interface is in processing communication with said PSD;

and wherein transmitting a second message from said PSD to said first remote computer system through said communications pipe comprises:

generating said second message in APDU format by said PSD

using a second internal PSD data processing means and transmitting said second APDU format message through said PSD Interface,

receiving by said client said second APDU format message through said PSD Interface and encapsulating said second APDU format message into said packet based communications protocol producing a second encapsulated message, using a second data processing means,

transmitting said second encapsulated message over said network using said packet based communications protocol,

receiving said second encapsulated message sent over said network by said remote computer system, processing said second encapsulated message using a third server data processing means to separate said second APDU message from said second encapsulated message thus generating a second ~~desencapsulated~~ decapsulated APDU message,

converting by said remote computer system said second ~~desencapsulated~~ decapsulated APDU message into a second message in a non-native protocol using a forth server data processing means, and forwarding said second message to at least one API Level Program;

generating an authentication challenge on said first remote

computer system in a proper format for processing by said PSD,

encrypting said properly formatted challenge using a pre-established cryptography method,

transmitting said encrypted challenge through said established communications pipe to said PSD,

decrypting said encrypted challenge by said PSD using said pre-established cryptography method,

generating an authentication response by said PSD using said decrypted challenge and at least one internal PSD algorithm,

encrypting said authentication response using said pre-established cryptography method,

transmitting said encrypted authentication response through said established communications pipe to said first remote computer system, and

decrypting said encrypted authentication response by said first remote computer system using said pre-established cryptography method and authenticating said response by said first remote computer system using at least one internal authentication algorithm.

8. (Previously Presented) The method according to claim 7, further comprising;

redirecting subsequent authentication challenges received over said network from a subsequent remote computer system to said first remote computer system,

processing said subsequent authentication challenges in said proper format for processing by said PSD through said established communications pipe,

encrypting said properly formatted challenge using said pre-established cryptography method,

transmitting said encrypted challenge through said established communications pipe to said PSD,

decrypting said encrypted challenge by said PSD using said pre-established cryptography method,

generating an authentication response by said PSD using said decrypted challenge and at least one internal PSD algorithm,

encrypting said authentication response using said pre-established cryptography method,

transmitting said encrypted authentication response through said established communications pipe to said first remote computer system,

decrypting said encrypted authentication response by said first remote computer system using said pre-established cryptography method, and

routing said authentication response over said network to said subsequent remote computer system, authenticating said response by said subsequent remote computer system using at least one internal authentication algorithms.

9. (Original) The method according to claim 7 wherein said communications is an open protocol.

10. (Original) The method according to claim 7 wherein said communications is a secure protocol.

11. (Original) The method according to claim 7 wherein said cryptography employs asynchronous methods.

12. (Original) The method according to claim 7 wherein said cryptography employs synchronous methods.

13. (Currently Amended) A method for providing authentication over a network using a pre-established communications pipe comprising:

establishing a communications pipe between a PSD and a first remote computer system over at least one network and using a client as a communications host for said PSD, wherein said

client and said first remote computer system are in functional communication using a packet based communications protocol over said network, wherein said PSD comprises an internal PSD algorithm, and wherein transmitting a first message from said first remote computer system to said PSD through said communications pipe comprises:

generating said first message on said first remote computer system, wherein said first message is in a non-native protocol for communicating with said PSD and said first message is generated by an API Level Program,

converting on said remote computer system said first message from said non-native protocol into a first APDU format message using a first server data processing means,

encapsulating on said first remote computer system said first APDU format message into said packet based communications protocol producing a first encapsulated message, using a second server data processing means,

transmitting said first encapsulated message over said network using said packet based communications protocol,

receiving by said client said first encapsulated message sent over said network, processing said first encapsulated message using a first data processing means to separate said first APDU format message from said first encapsulated message,

routing on said client said first APDU format message through a hardware device port assigned to a PSD Interface independently of the origin and integrity of said first encapsulated message, wherein said PSD Interface is in processing communication with said PSD;

and wherein transmitting a second message from said PSD to said first remote computer system through said communications pipe comprises:

generating said second message in APDU format by said PSD using a second internal PSD data processing means and transmitting said second APDU format message through said PSD Interface,

receiving by said client said second APDU format message through said PSD Interface and encapsulating said second APDU format message into said packet based communications protocol producing a second encapsulated message, using a second data processing means,

transmitting said second encapsulated message over said network using said packet based communications protocol,

receiving said second encapsulated message sent over said network by said remote computer system, processing said second encapsulated message using a third server data processing means to separate said second APDU message from said second

encapsulated message thus generating a second ~~desencapsulated~~ decapsulated APDU message,

converting by said remote computer system said second ~~desencapsulated~~ decapsulated APDU message into a second message in a non-native protocol using a forth server data processing means, and forwarding said second message to at least one API Level Program;

generating a command for requesting a transfer of said internal PSD algorithm, on a first remote computer system in a proper format for processing by said PSD,

encrypting said properly formatted transfer command using a pre-established cryptography method,

transmitting said encrypted transfer command through said established communications pipe to said PSD,

decrypting said encrypted transfer command by said PSD using said pre-established cryptography method,

copying said internal PSD algorithm into an internal memory location,

encrypting said internal PSD algorithm using said pre-established cryptography method,

transmitting said encrypted internal PSD algorithm through said established communications pipe to said first remote computer system,

decrypting said encrypted internal PSD algorithm by said first remote computer system using said pre-established cryptography method and storing said internal PSD algorithm in a secure location,

receiving at least one remote authentication challenge over said network from at least one subsequent remote computer system by said first remote computer system,

generating an authentication response by said first remote computer system using said stored internal PSD algorithm,

transmitting said generated authentication response over said network to said subsequent remote computer system, and

authenticating said response by said subsequent remote computer system using at least one internal authentication algorithm.

14. (Previously Presented) The method according to claim 13 wherein said communications is an open protocol.

15. (Previously Presented) The method according to claim 13 wherein said communications is a secure protocol.

16. (Previously Presented) The method according to claim 13 wherein said cryptography employs asynchronous methods.

17. (Previously Presented) The method according to claim 13 wherein said cryptography employs synchronous methods.